(f) DISPUTE RESOLUTION.—If there is a dispute between the Attor ney General and a telecommunications carrier regarding th amount of reasonable costs to be paid under subsection (a), the dis pute shall be resolved and the amount determined in a proceedin initiated at the Commission or by the court from which an enforce ment order is sought under section 2607.

* * * * * * *

§ 2703. Requirements for governmental access

(a) * * *

* * * * * * *

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVIC OR REMOTE COMPUTING SERVICE.—(1)(A) Except as provided i subparagraph (B), a provider of electronic communication service o remote computing service may disclose a record or other informa tion pertaining to a subscriber to or customer of such service (no including the contents of communications covered by subsection (a or (b) of this section) to any person other than a governmental en tity.

(B) A provider of electronic communication service or remot computing service shall disclose a record or other information pe taining to a subscriber to or customer or such service (not includin the contents of communications covered by subsection (a) or (b) this section) to a governmental entity only when the governmenta entity—

[(i) uses an administrative supoena authorized by a Feder or State statute, or a Federal or State grand jury or trail sul poena:]

[(ii)] *(i)* obtains a warrant issued under the Federal Rul of Criminal Procedure or equivalent State warrant;

[(iii)] *(ii)* obtains a court order for such disclosure und subsection (d) of this section; or

[(iv)] *(iii)* has the consent of the subscriber or customer such disclosure.

(C) A provider of electronic communication service or remote co puting service shall disclose to a governmental entity the name, a dress, telephone toll billing records, and length of service of a su scriber to or customer of such service and the types of services t subscriber or customer utilized, when the governmental entity us an administrative subpoena authorized by a Federal or State st ute or a Federal or State grand jury or trial subpoena or any mea available under subparagraph (B).

* * * * * * *

(d) REQUIREMENTS FOR COURT ORDER.—[A court order for disc sure under subsection (b) or (c) of this section may be issued by a court that is a court of competent jurisdiction set forth in secti 3126(2)(A) of this title and shall issue only if the governmental e tity shows that there is reason to believe the contents of a wire electronic communication, or the records or other informa sought, are relevant to a legitimate law enforcement inquiry.] *court order for disclosure under subsection (b) or (c) may be issu by any court that is a court of competent jurisdiction described*

section 3126(2)(A) and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

* * * * * * *

§ 3121. General prohibition on pen register and trap and trace device use; exception

(a) * * *

* * * * * * *

(c) LIMITATION.—A government agency authorized to install and use a pen register under this chapter or under State law, shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signalling information utilized in call processing.

[(c)] *(d)* PENALTY.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both

* * * * * * *

○

103D CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 103–827
Part 1

TELECOMMUNICATIONS CARRIER ASSISTANCE TO THE GOVERNMENT

OCTOBER 4, 1994.—Ordered to be printed

Mr. BROOKS, from the Committee on the Judiciary, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 4922]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 4922) to amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. INTERCEPTION OF DIGITAL AND OTHER COMMUNICATIONS.

(a) IN GENERAL.—Part I of title 18, United States Code, is amended by inserting after chapter 119 the following new chapter:

"CHAPTER 120—TELECOMMUNICATIONS CARRIER ASSISTANCE TO THE GOVERNMENT

"§ 2601. Definitions

"(a) DEFINITIONS.—In this chapter—

"the terms defined in section 2510 have, respectively, the meanings stated in that section.

"'call-identifying information'—

"(A) means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by the subscriber equipment, facility, or service of a telecommunications carrier that is the subject of a court order or lawful authorization; but

"(B) does not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number).

"'Commission' means the Federal Communications Commission.

"'government' means the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance.

"'information services'—

"(A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and

"(B) includes electronic publishing and electronic messaging services; but

"(C) does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network.

"'telecommunications support services' means a product, software, or service used by a telecommunications carrier for the internal signaling or switching functions of its telecommunications network.

"'telecommunications carrier'—

"(A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire (within the meaning of section 3(h) of the Communications Act of 1934 (47 U.S.C. 153(h))));

"(B) includes—

"(i) a person or entity engaged in providing commercial mobile service (as defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d))); or

"(ii) a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this chapter; but

"(C) does not include persons or entities insofar as they are engaged in providing information services.

"§ 2602. Assistance capability requirements

"(a) CAPABILITY REQUIREMENTS.—Except as provided in subsections (b), (c), and (d) of this section and sections 2607(c) and 2608(d), a telecommunications carrier shall ensure that its services or facilities that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of—

"(1) expeditiously isolating and enabling the government to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's service, facility, or equipment or at such later time as may be acceptable to the government;

"(2) expeditiously isolating and enabling the government to access call-identifying information that is reasonably available to the carrier—

"(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and

"(B) in a manner that allows it to be associated with the communication to which it pertains,

except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);

"(3) delivering intercepted communications and call-identifying information to the government in a format such that they may be transmitted by means of facilities or services procured by the government to a location other than the premises of the carrier; and

"(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects—

"(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and

"(B) information regarding the government's interception of communications and access to call-identifying information.

"(b) LIMITATIONS.—

"(1) DESIGN OF FEATURES AND SYSTEMS CONFIGURATIONS.—This chapter does not authorize any law enforcement agency or officer—

"(A) to require any specific design of features or system configurations to be adopted by providers of wire or electronic communication service, manufacturers of telecommunications equipment, or providers of telecommunications support services; or

"(B) to prohibit the adoption of any feature or service by providers of wire or electronic communication service, manufacturers of telecommunications equipment, or providers of telecommunications support services.

"(2) INFORMATION SERVICES; PRIVATE NETWORKS AND INTERCONNECTION SERVICES AND FACILITIES.—The requirements of subsection (a) do not apply to—

"(A) information services; or

"(B) services or facilities that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.

"(3) ENCRYPTION.—A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

"(c) EMERGENCY OR EXIGENT CIRCUMSTANCES.—In emergency or exigent circumstances (including those described in sections 2518 (7) or (11)(b) and 3125 of this title and section 1805(e) of title 50), a carrier at its discretion may comply with subsection (a)(3) by allowing monitoring at its premises if that is the only means of accomplishing the interception or access.

"(d) MOBILE SERVICE ASSISTANCE REQUIREMENTS.—A telecommunications carrier offering a feature or service that allows subscribers to redirect, hand off, or assign their wire or electronic communications to another service area or another service provider or to utilize facilities in another service area or of another service provider shall ensure that, when the carrier that had been providing assistance for the interception of wire or electronic communications or access to call-identifying information pursuant to a court order or lawful authorization no longer has access to the content of such communications or call-identifying information within the service area in which interception has been occurring as a result of the subscriber's use of such a feature or service, information is made available to the government (before, during, or immediately after the transfer of such communications) identifying the provider of wire or electronic communication service that has acquired access to the communications.

"§ 2603. Notices of capacity requirements

"(a) NOTICES OF MAXIMUM AND ACTUAL CAPACITY REQUIREMENTS.—

"(1) IN GENERAL.—Not later than 1 year after the date of enactment of this chapter, after consulting with State and local law enforcement agencies, telecommunications carriers, providers of telecommunications support services, and manufacturers of telecommunications equipment, and after notice and comment, the Attorney General shall publish in the Federal Register and provide to appropriate telecommunications industry associations and standard-setting organizations—

"(A) notice of the maximum capacity required to accommodate all of the communication interceptions, pen registers, and trap and trace devices that the Attorney General estimates that government agencies authorized to

conduct electronic surveillance may conduct and use simultaneously after the date that is 4 years after the date of enactment of this chapter; and

"(B) notice of the actual number of communication interceptions, pen registers, and trap and trace devices, representing a portion of the maximum capacity set forth under subparagraph (A), that the Attorney General estimates that government agencies authorized to conduct electronic surveillance may conduct and use simultaneously after the date that is 4 years after the date of enactment of this chapter.

"(2) BASIS OF NOTICES.—The notices issued under paragraph (1)—

"(A) may be based upon the type of equipment, type of service, number of subscribers, type or size or carrier, nature of service area, or any other measure; and

"(B) shall identify, to the maximum extent possible, the capacity required at specific geographic locations, including carrier office locations.

"(b) COMPLIANCE WITH CAPACITY NOTICES.—

"(1) INITIAL CAPACITY.—Within 3 years after the publication by the Attorney General of a notice of capacity requirements or within 4 years after the date of enactment of this chapter, whichever is longer, a telecommunications carrier shall, subject to subsection (e), ensure that its systems are capable of—

"(A) expanding to the maximum capacity set forth in the notice under subsection (a)(1)(A); and

"(B) accommodating simultaneously the number of interceptions, pen registers, and trap and trace devices set forth in the notice under subsection (a)(1)(B).

"(2) EXPANSION TO MAXIMUM CAPACITY.—After the date described in paragraph (1), a telecommunications carrier shall, subject to subsection (e), ensure that it can accommodate expeditiously any increase in the actual number of communication interceptions, pen registers, and trap and trace devices that authorized agencies may seek to conduct and use, up to the maximum capacity requirement set forth in the notice under subsection (a)(1)(A).

"(c) NOTICES OF INCREASED MAXIMUM CAPACITY REQUIREMENTS.—

"(1) The Attorney General shall periodically publish in the Federal Register, after notice and comment, notice of any necessary increases in the maximum capacity requirement set forth in the notice under subsection (a)(1)(A).

"(2) Within 3 years after notice of increased maximum capacity requirements is published under paragraph (1), or within such longer time period as the Attorney General may specify, a telecommunications carrier shall, subject to subsection (e), ensure that its systems are capable of expanding to the increased maximum capacity set forth in the notice.

"(d) CARRIER STATEMENT.—Within 180 days after the publication by the Attorney General of a notice of capacity requirements pursuant to subsection (a), a telecommunications carrier shall submit to the Attorney General a statement identifying any of its systems or services that do not have the capacity to accommodate simultaneously the number of interceptions, pen registers, and trap and trace devices set forth in the notice under subparagraph (A) or (B) of subsection (a)(1).

"(e) REIMBURSEMENT REQUIRED FOR COMPLIANCE.—The Attorney General shall review the statements submitted under subsection (d) and may, subject to the availability of appropriations, agree to reimburse a telecommunications carrier for the just and reasonable costs directly associated with modifications to attain such capacity requirement. Until the Attorney General agrees to reimburse such carrier for such modification, such carrier shall be considered to be in compliance with the capacity notices under subparagraphs (A) and (B) of subsection (a)(1).

"§ 2604. Systems security and integrity

"A telecommunications carrier shall ensure that any court ordered or lawfully authorized interception of communications or access to call-identifying information effected within its switching premises can be activated only with the affirmative intervention of an individual officer or employee of the carrier.

"§ 2605. Cooperation of equipment manufacturers and providers of telecommunications support services

"(a) CONSULTATION.—A telecommunications carrier shall consult, as necessary, in a timely fashion with manufacturers of its telecommunications transmission and switching equipment and its providers of telecommunications support services for the purpose of ensuring that current and planned services and equipment comply with the capability requirements of section 2602 and the capacity requirements identified by the Attorney General under section 2603.

"(b) COOPERATION.—Subject to sections 2607(c) and 2608(d), a manufacturer of telecommunications transmission or switching equipment and a provider of telecommunications support services shall, on a reasonably timely basis and at a reasonable charge, make available to the telecommunications carriers using its equipment or services such features or modifications as are necessary to permit such carriers to comply with the capability requirements of section 2602 and the capacity requirements identified by the Attorney General under section 2603.

"§ 2606. Technical requirements and standards; extension of compliance date

"(a) SAFE HARBOR.—

"(1) CONSULTATION.—To ensure the efficient and industry-wide implementation of the assistance capability requirements under section 2602, the Attorney General, in coordination with other Federal, State, and local law enforcement agencies, shall consult with appropriate associations and standard-setting organizations of the telecommunications industry and with representatives of users of telecommunications services and facilities.

"(2) COMPLIANCE UNDER ACCEPTED STANDARDS.—A telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 2602, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 2605, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization or by the Commission under subsection (b) to meet the requirements of section 2602.

"(3) ABSENCE OF STANDARDS.—The absence of technical requirements or standards for implementing the assistance capability requirements of section 2602 shall not—

"(A) preclude a carrier, manufacturer, or services provider from deploying a technology or service; or

"(B) relieve a carrier, manufacturer, or service provider of the obligations imposed by section 2602 or 2605, as applicable.

"(b) FCC AUTHORITY.—

"(1) IN GENERAL.—If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by notice and comment rulemaking or such other proceedings as the Commission may be authorized to conduct, technical requirements or standards that—

"(A) meet the assistance capability requirements of section 2602;

"(B) protect the privacy and security of communications not authorized to be intercepted; and

"(C) serve the policy of the United States to encourage the provision of new technologies and services to the public.

"(2) TRANSITION PERIOD.—If an industry technical requirement or standard is set aside or supplanted as a result of Commission action under this section, the Commission, after consultation with the Attorney General, shall establish a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 2602 during any transition period.

"(c) EXTENSION OF COMPLIANCE DATE FOR FEATURES AND SERVICES.—

"(1) PETITION.—A telecommunications carrier proposing to install or deploy or having installed or deployed, a feature or service within 4 years after the date of enactment of this chapter may petition the Commission for 1 or more extensions of the deadline for complying with the assistance capability requirements under section 2602.

"(2) GROUND FOR EXTENSION.—The Commission may, after affording a full opportunity for hearing and after consultation with the Attorney General, grant an extension under this paragraph, if the Commission determines that compliance with the assistance capability requirements under section 2602 is not reasonably achievable through application of technology available within the compliance period.

"(3) LENGTH OF EXTENSION.—An extension under this paragraph shall extend for no longer than the earlier of—

"(A) the date determined by the Commission as necessary for the carrier to comply with the assistance capability requirements under section 2602; or

"(B) the date that is 2 years after the date on which the extension is granted.

"(4) APPLICABILITY OF EXTENSION.—An extension under this subsection shall apply to only that part of the carrier's business on which the new feature or service is used.

"§ 2607. Enforcement orders

"(a) ENFORCEMENT BY COURT ISSUING SURVEILLANCE ORDER.—If a court authorizing an interception under chapter 119, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements in this chapter, the court may direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

"(b) ENFORCEMENT UPON APPLICATION BY ATTORNEY GENERAL.—The Attorney General may apply to the appropriate United States district court for, and the United States district courts shall have jurisdiction to issue, an order directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with this chapter.

"(c) GROUNDS FOR ISSUANCE.—A court shall issue an order under subsection (a) or (b) only if the court finds that—

"(1) alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement for implementing the interception of communications or access to call-identifying information; and

"(2) compliance with the requirements of this chapter is reasonably achievable through the application of available technology to the feature or service at issue or would have been reasonably achievable if timely action had been taken.

"(d) TIME FOR COMPLIANCE.—Upon issuance of an enforcement order under this section, the court shall specify a reasonable time and conditions for complying with its order, considering the good faith efforts to comply in a timely manner, any effect on the carrier's, manufacturer's, or service provider's ability to continue to do business, the degree of culpability or delay in undertaking efforts to comply, and such other matters as justice may require.

"(e) LIMITATION.—An order under this section may not require a telecommunications carrier to meet the government's demand for interception of communications and acquisition of call-identifying information to any extent in excess of the capacity for which the Attorney General has agreed to reimburse such carrier.

"(f) CIVIL PENALTY.—

"(1) IN GENERAL.—A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to $10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.

"(2) CONSIDERATIONS.—In determining whether to impose a fine and in determining its amount, the court shall take into account—

"(A) the nature, circumstances, and extent of the violation;

"(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and

"(C) such other matters as justice may require.

"(3) CIVIL ACTION.—The Attorney General may file a civil action in the appropriate United States district court to collect, and the United States district courts shall have jurisdiction to impose, such fines.

"§ 2608. Payment of costs of telecommunications carriers to comply with capability requirements

"(a) EQUIPMENT, FEATURES, AND SERVICES DEPLOYED BEFORE DATE OF ENACTMENT.—The Attorney General may, subject to the availability of appropriations, agree to pay telecommunications carriers for all just and reasonable costs directly associated with the modifications performed by carriers in connection with equipment, features, and services installed or deployed before the date of enactment of this chapter to establish the capabilities necessary to comply with section 2602.

"(b) EQUIPMENT, FEATURES, AND SERVICES DEPLOYED ON OR AFTER DATE OF ENACTMENT.—

"(1) IN GENERAL.—If compliance with the assistance capability requirements of section 2602 is not reasonably achievable with respect to equipment, features or services deployed on or after the date of enactment of this chapter, the Attorney General, on application of a telecommunications carrier, may agree to pay the telecommunications carrier for just and reasonable costs directly associated with achieving compliance.

"(2) CONSIDERATION.—In determining whether compliance with the assistance capability requirements of section 2602 is reasonably achievable with respect to any equipment, feature, or service installed or deployed after the date of enactment of this chapter, consideration shall be given to the time when the equipment, feature, or service was installed or deployed.

"(c) ALLOCATION OF FUNDS FOR PAYMENT.—The Attorney General shall allocate funds appropriated to carry out this chapter in accordance with law enforcement priorities determined by the Attorney General.

"(d) FAILURE TO MAKE PAYMENT WITH RESPECT TO EQUIPMENT, FEATURES, AND SERVICES DEPLOYED BEFORE DATE OF ENACTMENT.—

"(1) CONSIDERED TO BE IN COMPLIANCE.—If a carrier has requested payment in accordance with procedures promulgated pursuant to subsection (e), and the Attorney General has not agreed to pay the telecommunications carrier for all reasonable costs directly associated with modifications necessary to bring the equipment, feature, or service into actual compliance with the assistance capability requirements of section 2602, any equipment, feature, or service of a telecommunications carrier deployed before the date of enactment of this chapter shall be considered to be in compliance with the assistance capability requirements of section 2602 until the equipment, feature, or service is replaced or significantly upgraded or otherwise undergoes major modification.

"(2) LIMITATION ON ORDER.—An order under section 2607 shall not require a telecommunications carrier to modify, for the purpose of complying with the assistance capability requirements of section 2602, any equipment, feature, or service deployed before the date of enactment of this chapter unless the Attorney General has agreed to pay the telecommunications carrier for all just and reasonable costs directly associated with modifications necessary to bring the equipment, feature, or service into actual compliance with those requirements.

"(e) PROCEDURES AND REGULATIONS.—Notwithstanding any other law, the Attorney General shall, after notice and comment, establish any procedures and regulations deemed necessary to effectuate timely and cost-efficient payment to telecommunications carriers for compensable costs incurred under this chapter, under chapters 119 and 121, and under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(f) DISPUTE RESOLUTION.—If there is a dispute between the Attorney General and a telecommunications carrier regarding the amount of just and reasonable costs to be paid under subsection (a), the dispute shall be resolved and the amount determined in a proceeding initiated at the Commission or by the court from which an enforcement order is sought under section 2607.".

(b) TECHNICAL AMENDMENT.—The part analysis for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 119 the following new item:

"120. Telecommunications carrier assistance to the Government ..... 2601"

SEC. 2. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to carry out section 2608 of title 18, United States Code, as added by section 1—

(1) a total of $500,000,000 for fiscal years 1995, 1996, and 1997; and

(2) such sums as are necessary for each fiscal year thereafter,

such sums to remain available until expended.

SEC. 3. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in paragraph (2), chapter 120 of title 18, United States Code, as added by section 1, shall take effect on the date of enactment of this Act.

(b) ASSISTANCE CAPABILITY AND SYSTEMS SECURITY AND INTEGRITY REQUIREMENTS.—Sections 2602 and 2604 of title 18, United States Code, as added by section 1, shall take effect on the date that is 4 years after the date of enactment of this Act.

SEC. 4. REPORTS.

(a) REPORTS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—On or before November 30, 1995, and on or before November 30 of each year for 5 years thereafter, the Attorney General shall submit to Congress and make available to the public a report on the amounts paid during the preceding fiscal year in payment to telecommunications carriers under section 2608 of title 18, United States Code, as added by section 1.

(2) CONTENTS.—A report under paragraph (1) shall include—

(A) a detailed accounting of the amounts paid to each carrier and the technology, equipment, feature or service for which the amounts were paid; and

(B) projections of the amounts expected to be paid in the current fiscal year, the carriers to which payment is expected to be made, and the technologies, equipment, features or services for which payment is expected to be made.

(b) REPORTS BY THE COMPTROLLER GENERAL.—

(1) PAYMENTS FOR MODIFICATIONS.—On or before April 1, 1996, and April 1, 1998, the Comptroller General of the United States, after consultation with the Attorney General and the telecommunications industry, shall submit to the Congress a report reflecting its analysis of the reasonableness and cost-effectiveness of the payments made by the Attorney General to telecommunications carriers for modifications necessary to ensure compliance with chapter 120 of title 18, United States Code, as added by section 1.

(2) COMPLIANCE COST ESTIMATES.—A report under paragraph (1) shall include the findings and conclusions of the Comptroller General on the costs to be incurred after the compliance date, including projections of the amounts expected to be incurred and the technologies, equipment, features or services for which expenses are expected to be incurred by telecommunications carriers to comply with the assistance capability requirements in the first 5 years after the effective date of section 2602.

SEC. 5. CORDLESS TELEPHONES.

(a) DEFINITIONS.—Section 2510 of title 18, United States Code, is amended—

(1) in paragraph (1) by striking ", but such term does not include" and all that follows through "base unit"; and

(2) in paragraph (12) by striking subparagraph (A) and redesignating subparagraphs (B), (C), and (D) as subparagraphs (A), (B), and (C), respectively.

(b) PENALTY.—Section 2511 of title 18, United States Code, is amended—

(1) in subsection (4)(b)(i) by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,"; and

(2) in subsection (4)(b)(ii) by inserting "a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit," after "cellular telephone communication,".

SEC. 6. RADIO-BASED DATA COMMUNICATIONS.

Section 2510(16) of title 18, United States Code, is amended—

(1) by striking "or" at the end of subparagraph (D);

(2) by inserting "or" at the end of subparagraph (E); and

(3) by inserting after subparagraph (E) the following new subparagraph:

"(F) an electronic communication;"

SEC. 7. PENALTIES FOR MONITORING RADIO COMMUNICATIONS THAT ARE TRANSMITTED USING MODULATION TECHNIQUES WITH NONPUBLIC PARAMETERS.

Section 2511(4)(b) of title 18, United States Code, is amended by striking "or encrypted, then" and inserting ", encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication".

SEC. 8. TECHNICAL CORRECTION.

Section 2511(2)(a)(i) of title 18, United States Code, is amended by striking "used in the transmission of a wire communication" and inserting "used in the transmission of a wire or electronic communication".

SEC. 9. FRAUDULENT ALTERATION OF COMMERCIAL MOBILE RADIO INSTRUMENTS.

(a) OFFENSE.—Section 1029(a) of title 18, United States Code, is amended—

(1) by striking "or" at the end of paragraph (3); and

(2) by inserting after paragraph (4) the following new paragraphs:

"(5) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services; or

"(6) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses—

"(A) a scanning receiver; or

"(B) hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services.".

(b) PENALTY.—Section 1029(c)(2) of title 18, United States Code, is amended by striking "(a)(1) or (a)(4)" and inserting "(a)(1), (4), (5), or (6)".

(c) DEFINITIONS.—Section 1029(e) of title 18, United States Code, is amended—

(1) in paragraph (1) by inserting "electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier," after "account number,";

(2) by striking "and" at the end of paragraph (5);

(3) by striking the period at the end of paragraph (6) and inserting ", and"; and

(4) by adding at the end the following new paragraph:

"(7) the term 'scanning receiver' means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119."

SEC. 10. TRANSACTIONAL DATA.

(a) DISCLOSURE OF RECORDS.—Section 2703 of title 18, United States Code, is amended—

(1) in subsection (c)(1)—

(A) in subparagraph (B)—

(i) by striking clause (i); and

(ii) by redesignating clauses (ii), (iii), and (iv) as clauses (i), (ii), and (iii), respectively; and

(B) by adding at the end the following new subparagraph:

"(C) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the name, address, telephone toll billing records, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under subparagraph (B).";

(2) by amending the first sentence of subsection (d) to read as follows: "A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction described in section 3126(2)(A) and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.".

(b) PEN REGISTERS AND TRAP AND TRACE DEVICES.—Section 3121 of title 18, United States Code, is amended—

(1) by redesignating subsection (c) as subsection (d); and

(2) by inserting after subsection (b) the following new subsection:

"(c) LIMITATION.—A government agency authorized to install and use a pen register under this chapter or under State law, shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.".

SUMMARY AND PURPOSE

The purpose of H.R. 4922 is to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services.

To insure that law enforcement can continue to conduct authorized wiretaps in the future, the bill requires telecommunications carriers to ensure their systems have the capability to: (1) isolate expeditiously the content of targeted communications transmitted by the carrier within the carrier's service area; (2) isolate expedi-

tiously information identifying the origin and destination of targeted communications; (3) provide intercepted communications and call identifying information to law enforcement so they can be transmitted over lines or facilities leased by law enforcement to a location away from the carrier's premises; and (4) carry out intercepts unobtrusively, so targets are not made aware of the interception, and in a manner that does not compromise the privacy and security of other communications. The bill allows industry to develop standards to implement these requirements. It establishes a process for the Attorney General to identify capacity requirements.

In recognition of the fact that some existing equipment, services or features will have to be retrofitted, the legislation provides that the Federal government will pay carriers for just and reasonable costs incurred in modifying existing equipment, services or features to comply with the capability requirements. The legislation also provides that the government will pay for expansions in capacity to accommodate law enforcement needs.

The legislation also expands privacy and security protection for telephone and computer communications. The protections of the Electronic Communications Privacy Act of 1986 are extended to cordless phones and certain data communications transmitted by radio. In addition, the bill increases the protection for transactional data on electronic communications services by requiring law enforcement to obtain a court order for access to electronic mail addressing information.

The bill further protects privacy by requiring the systems of telecommunications carriers to protect communications not authorized to be intercepted and by restricting the ability of law enforcement to use pen register devices for tracking purposes or for obtaining transactional information. Finally, the bill improves the privacy of mobile phones by expanding criminal penalties for using certain devices to steal mobile phone service.

HEARINGS

In the 103d Congress, the Subcommittee on Civil and Constitutional Rights held two joint hearings with the Senate Judiciary Subcommittee on Technology and the Law on the impact of advanced telecommunications services and technologies on electronic surveillance, March 18 and August 11, 1994.

At the first hearing, held before legislation was introduced, the witnesses were Louis J. Freeh, Director of the Federal Bureau of Investigation; William C. O'Malley, district attorney for Plymouth County, Massachusetts, and President of the National District Attorneys Association; Roy Neel, President of the United States Telephone Association, which represents local telephone companies ranging in size from the Regional Bell Operating Companies ("RBOCs") to small companies with fewer than 100 subscribers; and Jerry Berman, Executive Director of the Electronic Frontier Foundation ("EFF"), on behalf of EFF and the Digital Privacy and Security Working Group, a coalition of computer, communications, and public interest organizations and associations.

The second hearing was held after the introduction of H.R. 4922. Again, Director Freeh, Mr. Neel, and Mr. Berman appeared and presented testimony. Also appearing as witnesses were Hazel Ed-

wards, Director, Information Resources Management/General Government, Accounting and Information Management Division, U.S. General Accounting Office; and Thomas E. Wheeler, President and CEO of the Cellular Telecommunications Industry Association, which represents providers of two-way wireless telecommunications services, including licensed cellular, personal communications services, and enhanced specialized mobile radio.

Written submissions for the record were received from AT&T Corporation, MCI Communications Corporation, the Telecommunications Industry Association, which represents U.S. manufacturers of telecommunications equipment, the National Sheriffs' Association, the National Association of Attorneys General, and the Major Cities Chiefs, an organization of police executives representing the 49 largest metropolitan areas in the U.S. and Canada.

SUBCOMMITTEE ACTION

On August 17, 1994, the Subcommittee on Civil and Constitutional Rights, by voice vote, a reporting quorum being present, ordered favorably reported the bill H.R. 4922 without amendment.

COMMITTEE ACTION

On September 29, 1994, the Committee, by voice vote, a reporting quorum being present, adopted an amendment in the nature of a substitute to H.R. 4922 and ordered the bill favorably reported as amended.

BACKGROUND AND DISCUSSION

For the past quarter century, the law of this nation regarding electronic surveillance has sought to balance the interests of privacy and law enforcement. In 1968, the enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 simultaneously outlawed the use of electronic surveillance by private parties and authorized its use pursuant to a court order by law enforcement officials engaged in the investigation of specified types of major crimes. The Senate Report on Title III stated explicitly that the legislation "has as its dual purpose (1) protecting the privacy of wire and oral communications and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." Senate Committee on the Judiciary, Omnibus Crime Control and Safe Streets Act of 1967, S. Rep. No. 1097, 90th Cong., 2d Sess. (1968) at 66.

Congress was prompted to act in 1968 in part by advancements in technology, which posed a threat to privacy. According to the 1968 Report, "[t]he tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communication is seriously jeopardized by these techniques of surveillance." Id. at 67.

After 1968, telecommunications technology continued to change and again Congress was required to respond legislatively to preserve the balance between privacy and law enforcement. In the

Electronic Communications Privacy Act of 1986 ("ECPA"), Congress extended the privacy protections and the law enforcement intercept authority of Title III to a new set of technologies and services such as electronic mail, cellular telephones and paging devices. Again, the goal of the legislation was to preserve "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement." House Committee on the Judiciary, Electronic Communications Privacy Act of 1986, H. Rep. 99–647, 99th Cong. 2d Sess. 2 (1986) at 19.

Law enforcement officials have consistently testified, as Director Freeh did at the hearings of the bill, that court-authorized electronic surveillance is a critical law enforcement and public safety tool.

CONGRESS MUST RESPOND TO THE "DIGITAL TELEPHONY" REVOLUTION

Telecommunications, of course, did not stand still after 1986. Indeed, the pace of change in technology and in the structure of the telecommunications industry accelerated and continues to accelerate. The resulting challenges for law enforcement and privacy protection have sometimes been encapsulated under the rubric "digital telephony," but the issues go far beyond the distribution between analog and digital transmission modes. Some of the problems encountered by law enforcement relate to the explosive growth of cellular and other wireless services, which operate in both analog and digital modes. Other impediments to authorized wiretaps, like call forwarding, have long existed in the analog environment. Other considerations, such as the increasing amount of transactional data generated by the millions of users of on-line services, highlight the ever increasing opportunities for loss of privacy.

In 1990, Senator Patrick Leahy, chairman of the Senate Judiciary Subcommittee on Technology and the Law, assembled a Privacy and Technology Task Force with experts from business, consumer advocacy, the law, and civil liberties, to examine current developments in communications technology and the extent to which the law in general, and ECPA, specifically, protected, or failed adequately to protect, personal and corporate privacy.

After examining a wide array of communication media, including cellular phones, personal communications networks, the newer generation of cordless phones, wireless modems, wireless local area networks (LANs), and electronic mail and messaging, the task force issued a final report on May 28, 1991 recommending, inter alia, that the legal protections of ECPA be extended to cover new wireless data communications, such as those occurring over cellular laptop computers and wireless local area networks (LANs), and cordless phones. In addition, the Task Force found that ECPA was serving well its purpose of protecting the privacy of the contents of electronic mail, but questioned whether current restrictions on government access to transactional records generated in the course of electronic communications were adequate.

Consistent with the task force's conclusions and in view of the increasing impediments to authorized law enforcement electronic surveillance, the Committee has concluded that continued change in the telecommunications industry deserves legislative attention to preserve the balance sought in 1968 and 1986. However, it became

clear to the Committee early in its study of the "digital telephony" issue that a third concern now explicitly had to be added to the balance, namely, the goal of ensuring that the telecommunications industry was not hindered in the rapid development and deployment of the new services and technologies that continue to benefit and revolutionize society.

Therefore, the bill seeks to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.

THE PROBLEM: LEGISLATION NEEDED TO CLARIFY CARRIERS' DUTY TO COOPERATE

When originally enacted, Title III contained no provision specifically addressing what responsibility, if any, telecommunications carriers and others had to assist law enforcement in making authorized interceptions. Shortly after the statute became effective, the FBI asked a local telephone company to assist in effectuating an authorized wiretap by providing leased lines and connecting bridges. The telephone company refused and in 1970 the U.S. Court of Appeals for the Ninth Circuit held that, absent carriers to assist lawful wiretaps. *Application of the United States*, 427 F.2d 639 (9th Cir. 1970). Two months after the Ninth Circuit decision and with little debate, Congress added to 18 U.S.C. 2518(4) a provision that now reads:

> An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.

While the Supreme Court has read this provision as requiring the Federal courts to compel, upon request of the government, "any assistance necessary to accomplish an electronic interception, *United States* v. *New York Telephone*, 434 U.S. 159, 177 (1977), the question of whether companies have any obligation to design their systems such that they do not impede law enforcement interception has never been adjudicated.

Indeed, until recently, the question of system design was never an issue for authorized surveillance, since intrinsic elements of wire lined networks presented access points where law enforcement, with minimum assistance from telephone companies, could

isolate the communications associated with a particular surveillance target and effectuate an intercept. Where problems did arise, they could be addressed on a case-by-case basis in negotiations between the local monopoly service provider and law enforcement. (From a public policy perspective, such arrangements would have had the disadvantage of being concluded without public knowledge or legislative oversight.)

The break-up of the Bell system and the rapid proliferation of new telecommunications technologies and services have vastly complicated law enforcement's task in that regard. The goal of the legislation, however, is not to reverse those industry trends. Indeed, it is national policy to promote competition in the telecommunications industry and to support the development and widespread availability of advanced technologies, features and services. The purpose of the legislation is to further define the industry duty to cooperate and to establish procedures based on public accountability and industry standards-setting.

The Committee has concluded that there is sufficient evidence justifying legislative action that new and emerging telecommunications technologies pose problems for law enforcement. The evidence comes from three sources: the General Accounting Office, the FBI, and the telecommunications industry itself.

GAO findings

In 1992, analysts from the GAO's Information Management and Technology Division interviewed technical representatives from local telephone companies, switch manufacturers, and cellular providers, as well as the FBI. The GAO found that the FBI had not adequately defined its electronic surveillance requirements, but the GAO concluded that law enforcement agencies did have technical problems tapping a variety of services or technologies, including call forwarding, fiber, and ISDN. The GAO also concluded that cellular systems could be tapped but that capacity was limited.

The GAO recently conducted further work and testified at the hearing on August 11, 1994. The GAO reconfirmed its earlier conclusion that there are legitimate impediments posed by new and emerging technologies. The GAO also concluded that the FBI had made progress in defining law enforcement's needs in terms of capability and capacity.

FBI survey

FBI Director Freeh testified at the March 18, 1994, hearing that the FBI had identified specific instances in which law enforcement agencies were precluded due to technological impediments from fully implementing authorized electronic surveillance (wiretaps, pen registers and trap and traces). The Director testified in March that an informal FBI survey of federal, state, and local law enforcement agencies had identified 91 such incidents, 33% of which involved cellular systems (11% were related to the limited capacity of cellular systems to accommodate a large number of intercepts simultaneously) and 32% of which involved custom calling features such as call forwarding, call waiting and speed dialing.

Because the existence of a problem continued to be questioned by some, the FBI re-contacted law enforcement agencies after the

March hearing and identified further examples. In April, 1994, the FBI presented to the House and Senate Judiciary Subcommittees details of 183 instances (including the original 91) where the FBI, State or local agencies had encountered problems. This evidence was presented to the Subcommittees on the understanding that the details would not be publicly disseminated. However, the following chart summarizes the FBI's findings:

Technology-based problems encountered by Federal, State, and local law enforcement agencies

	Page 183
Total problems	
Cellular port capacity	54
Inability to capture dialed digits contemporaneous with audio	33
Cellular provider could not intercept long-distance calls (or provide call setup information) to or from a targeted phone	4
Speed dialing/voice dialing/call waiting	20
Call forwarding	10
Direct inward dial trunk group (provider unable to isolate target's communications or provide call set-up information to the exclusion of all other customers)	4
Voice mail (provider unable to provide access to the subject's audio when forwarded to voice mail or retrieve messages)	12
Digital Centrex (provider unable to isolate all communications associated with the target to the exclusion of all others)	4
Other (including other calling features such as Call Back; and provider unable to: provide trap and trace information; isolate the digital transmissions associated with a target to the exclusion of all other communications; comprehensively intercept communications and provide call set-up information)	42

Industry acknowledges the problem

Representatives of the telecommunications industry now acknowledge that there will be increasingly serious problems for law enforcement interception posed by new technologies and the new competitive telecommunications market. At the hearing on August 11, Roy Neel, president of the United States Telephone Association and the chief spokesperson for the telephone industry on this issue, was asked by Senator Leahy if the time was fast approaching when a great deal of the ability of law enforcement to carry out wiretaps will be lost. Mr. Neel answered, "In a number of cases with new enhanced services, that is probably true."

The industry maintains that its companies have a long tradition of working with law enforcement under current law to resolve technical issues. However, with the proliferation of services and service providers, such a company-by-company approach is becoming increasingly untenable.

In response, the phone companies and the FBI have created an Electronic Communications Service Provider Committee, through which representatives of all the RBOCs have been meeting with law enforcement on a regular basis to develop solutions to a range of problems. The committee has created "Action Teams" on personal communications services, wireless cellular, the "advanced intelligence network," and switch-based solutions, among others. The chairman of the committee, a vice president of one of the RBOCs, stated in a letter dated March 1 and submitted by the FBI Director during his testimony in March: "If meaningful solutions are to result, all participants must first understand that there is in fact a

problem, not that one participant, or one group of participants, says so. Now that the Committee recognizes the problems, it can proceed to identify and develop appropriate solutions."

However, participation in the Service Provider Committee is voluntary and its recommendations are unenforceable. As a result, the Judiciary Committee has concluded that legislation is necessary.

LAW ENFORCEMENT REQUIREMENTS

The legislation requires telecommunications common carriers to ensure that new technologies and services do not hinder law enforcement access to the communications of a subscriber who is the subject of a court order authorizing electronic surveillance. The bill will preserve the government's ability, pursuant to court order, to intercept communications that utilize advanced technologies such as digital or wireless transmission.

To insure that law enforcement can continue to conduct wiretaps, the bill requires telecommunications carriers to ensure their systems have the capability to:

(1) Isolate expeditiously the content of targeted communications transmitted within the carrier's service area;

(2) Isolate expeditiously information identifying the originating and destination numbers of targeted communications, but not the physical location of targets;

(3) Provide intercepted communications and call identifying information to law enforcement in a format such that they may be transmitted over lines or facilities leased by law enforcement to a location away from the carrier's premises; and

(4) Carry out intercepts unobtrusively, so targets of electronic surveillance are not made aware of the interception, and in a manner that does not compromise the privacy and security of other communications.

Cost

The GAO testified at the August 11, 1994 hearing that the costs of compliance with the foregoing will depend largely on the details of standards and technical specifications, which, under the bill, will be developed over the next four years by industry associations and standard-setting organizations.

The bill requires the Federal government, with appropriated funds, to pay all reasonable costs incurred by industry over the next four years to retrofit existing facilities to bring them into compliance with the interception requirements. The bill authorizes at least $500 million for this purpose. In the event that the $500 million is not enough or is not appropriated, the legislation provides that any equipment, features or services deployed on the date of enactment, which government does not pay to retrofit, shall be considered to be in compliance until the equipment, feature, or service is replaced or significantly upgraded or otherwise undergoes major modification.

After the four year transition period, which may be extended an additional two years by order of the FCC, industry will bear the cost of ensuring that new equipment and services meet the legislated requirements, as defined by standards and specifications promulgated by the industry itself.

However, to the extent that industry must install additional capacity to meet law enforcement needs, the bill requires the government to pay all capacity costs from date of enactment, including all capacity costs incurred after the four year transition period. The Federal government, in its role of providing technical support to state and local law enforcement, will pay costs incurred in meeting the initial capacity needs and the future maximum capacity needs for electronic surveillance at all levels of government.

THE LEGISLATION ADDRESSES PRIVACY CONCERNS

Since 1968, the law of this nation has authorized law enforcement agencies to conduct wiretaps pursuant to court order. That authority extends to voice, data, fax, E-mail and any other form of electronic communication. The bill will not expand that authority. However, as the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited.

In the eight years since the enactment of ECPA, society's patterns of using electronic communications technology have changed dramatically. Millions of people now have electronic mail addresses. Business, nonprofit organizations and political groups conduct their work over the Internet. Individuals maintain a wide range of relationships on-line. Transactional records documenting these activities and associations are generated by service providers. For those who increasingly use these services, this transactional data reveals a great deal about their private lives, all of it compiled in one place.

In addition, while the portion of cordless telephone communications occurring between the handset and base unit was excluded from ECPA's privacy protections, the 1991 Privacy and Technology Task Force found that "[t]he cordless phone, far from being a novelty item used only at 'poolside,' has become ubiquitous . . . More and more communications are being carried out by people [using cordless phones] in private, in their homes and offices, with an expectation that such calls are just like any other phone call."

Therefore, H.R. 4922 includes provisions, which FBI Director Freeh supported in his testimony, that add protections to the exercise of the government's current surveillance authority. Specifically, the bill:

1. Eliminates the use of subpoenas to obtain E-mail addresses and other similar transactional data from electronic communications service providers. Currently, the government can obtain transactional logs containing a person's entire on-line profile merely upon presentation of an administrative subpoena issued by an investigator without any judicial intervention. Under H.R. 4922, a court order would be required.

2. Expressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information, other than that which can be determined from the phone number. Currently, in some cellular systems, transactional data that could be obtained by a pen register may include location information. Further, the bill requires law enforcement to use reasonably available technology to minimize information obtained through pen registers.

3. Explicitly states that it does not limit the rights of subscribers to use encryption.

4. Allows any person, including public interest groups, to petition the FCC for review of standards implementing wiretap capability requirements, and provides that one factor for judging those standards is whether they protect the privacy of communications not authorized to be intercepted.

5. Does not require mobile service providers to reconfigure their networks to deliver the content of communications occurring outside a carrier's service area.

6. Extends privacy protections of the Electronic Communications Privacy Act to cordless phones and certain data communications transmitted by radio.

7. Requires affirmative intervention of common carriers' personnel for switch-based interceptions—this means law enforcement will not be able to activate interceptions remotely or independently within the switching premises of a telecommunications carrier.

Narrow scope

It is also important from a privacy standpoint to recognize that the scope of the legislation has been greatly narrowed. The only entities required to comply with the functional requirements are telecommunications common carriers, the components of the public switched network where law enforcement agencies have always served most of their surveillance orders. Further, such carriers are required to comply only with respect to services or facilities that provide a customer or subscriber with the ability to originate, terminate or direct communications.

The bill is clear that telecommunications services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers (these would include long distance carriage) need not meet any any wiretap standards. PBXs are excluded. So are automated teller machine (ATM) networks and other closed networks. Also excluded from coverage are all information services, such as Internet service providers or services such as Prodigy and America-On-Line.

All of these private network systems or information services can be wiretapped pursuant to court order, and their owners must cooperate when presented with a wiretap order, but these services and systems do not have to be designed so as to comply with the capability requirements. Only telecommunications carriers, as defined in the bill, are required to design and build their switching and transmission systems to comply with the legislated requirements. Earlier digital telephony proposals covered all providers of electronic communications services, which meant every business and institution in the country. That broad approach was not practical. Nor was it justified to meet any law enforcement need.

H.R. 4922 RESPONDS TO INDUSTRY CONCERNS

H.R. 4922 includes several provisions intended to ease the burden on industry. The bill grants telephone companies and other covered entities a *four* year transition period in which to make any necessary changes in their facilities. In addition, it allows any com-

pany to seek from the FCC up to a two year extension of the compliance date if retrofitting a particular system will take longer than the four years allowed for compliance.

The Federal government will pay will reasonable costs incurred by industry in retrofitting facilities to correct existing problems.

The bill requires the Attorney General to estimate the capacity needs of law enforcement for electronic surveillance, so that carriers will have notice of what the government is likely to request. The bill requires government to reimburse carriers for reasonable costs of expanding capacity to meet law enforcement needs.

No impediment to technological innovation

The Committee's intent is that compliance with the requirements in the bill will not impede the development and deployment of new technologies. The bill expressly provides that law enforcement may not dictate system design features and may not bar introduction of new features and technologies. The bill establishes a reasonableness standard for compliance of carriers and manufacturers. Courts may order compliance and may bar the introduction of technology, but only if law enforcement has no other means reasonably available to conduct interception *and if* compliance with the standards is reasonably achievable through application of available technology. This means that if a service of technology *cannot* reasonably be brought into compliance with the interception requirements, then the service or technology *can* be deployed. This is the exact opposite of the original versions of the legislation, which would have barred introduction of services or features that could not be tapped. One factor to be considered when determining whether compliance is reasonable is the cost to the carrier of compliance compared to the carrier's overall cost of developing or acquiring and deploying the feature or service in question.

The legislation provides that the telecommunications industry itself shall decide how to implement law enforcement's requirements. The bill allows industry associations and standard-setting bodies, in consultation with law enforcement, to establish publicly available specifications creating "safe harbors" for carriers. This means that those whose competitive future depends on innovation will have a key role in interpreting the legislated requirements and finding ways to meet them without impeding the deployment of new services. If industry associations or standard-setting organizations fail to issue standards to implement the capability requirements, or if a government agency or any person, including a carrier, believes that such requirements or standards are deficient, the agency or person may petition the FCC to establish technical requirements or standards.

Accountability

Finally the bill has a number of mechanisms that will allow for Congressional and public oversight. The bill requires the government to estimate its capacity needs and publish them in the Federal Register. the bill requires the government, with funds appropriated by Congress through the normal appropriations process, to pay all reasonable costs incurred by industry in retrofitting facilities to correct existing problems. It requires the Attorney General

to file yearly reports on these expenditures for the first six years after date of enactment, and requires reports from the General Accounting Office in 1996 and 1998 estimating future costs of compliance. It requires that the government to reimburse carriers, with publicly appropriated funds, in perpetuity for the costs of expanding capacity to meet law enforcement needs. Furthermore, all proceedings before the FCC will be subject to public scrutiny, as well as congressional oversight ad judicial review.

RELATIONSHIP WITH EXISTING ASSISTANCE REQUIREMENTS

The assistance capability and capacity requirements of the bill are in addition to the existing necessary assistance requirements in sections 2518(4) and 3124 of title 18, and 1805(b) of title 50. The Committee intends that 2518(4), 3124, and 1805(b) will continue to be applied, as they have in the past, to government assistance requests related to specific orders, including, for example, the expenses of leased lines.

SECTION-BY-SECTION ANALYSIS

SECTION 1.—INTERCEPTION OF DIGITAL AND OTHER COMMUNICATIONS

This section adds a new chapter 120 to title 18, United States code, to define more precisely the assistance that telecommunications carriers are required to provide in connection with court orders for wire and electronic interceptions, pen registers and trap and trace devices. This new chapter contains eight sections numbered 2601 through 2608.

Section 2601 provides definitions for "call-identifying information," "information services," "government," "telecommunication support services," "telecommunications carrier."

A "telecommunications carrier" is defined as any person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire, as defined by section 3(h) of the Communications Act of 1934, and includes a commercial mobile service, as defined in section 332(d) of the Communications Act, as amended. This definition encompasses such service providers as local exchange carriers, interexchange carriers, competitive access providers (CAPs), cellular carriers, providers of personal communications services (PCS), satellite-based service providers, cable operators and electric or other utilities that provide telecommunications services for hire to the public, and any other common carrier that offers wireline or wireless service for hire to the public. The definition of telecommunications carrier does not include persons or entities to the extent they are engaged in providing information services, such as electronic mail providers, on-line services providers, such as Compuserve, Prodigy, America-On-line or Mead Data, or Internet service providers. Call forwarding, speed dialing, and the call redirection portion of a voice mail service are covered by the bill.

In addition, for purposes of this bill, the FCC is authorized to deem other persons and entities to be telecommunications carriers subject to the assistance capability and capacity requirements to the extent that such person or entity serves as a replacement for the local telephone service to a substantial portion of the public

within a state. As part of its determination whether the public interest is served by deeming a person or entity a telecommunications carrier for the purposes of this bill, the Commission shall consider whether such determination would promote competition, encourage the development of new technologies, and protect public safety and national security.

The term "call-identifying information" means the dialing or signaling information generated that identifies the origin and destination or a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization. For voice communications, this information is typically the electronic pulses, audio tones, or signalling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carrier's network. In pen register investigations, these pulses, tones, or messages identify the numbers dialed from the facility that is the subject of the court order or other lawful authorization. In trap and trace investigations, these are the incoming pulses, tones, or messages which identify the originating number of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order or authorization. Other dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information.

The term "government" means the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance.

The term "telecommunications support services" means a product, software or service used by a telecommunications carrier for the internal signaling or switching functions of its telecommunications network. The Committee understands there are currently over one hundred entities that provide common carriers with specialized support services. The definition of "telecommunications support services" excludes "information services," as defined in the bill.

The term "information services" includes messaging services offered through software such as groupware and enterprise or personal messaging software, that is, services based on products (including but not limited to multimedia software) of which Lotus Notes (and Lotus Network Notes), Microsoft Exchange Server, Novell Netware, CC: Mail, MCI Mail, Microsoft Mail, Microsoft Exchange Server, and AT&T Easylink (and their associated services) are both examples and precursors. It is the Committee's intention not to limit the definition of "information services" to such current services, but rather to anticipate the rapid development of advanced software and to include such software services in the definition of "information services." By including such software-based electronic messaging services within the definition of information services, they are excluded from compliance with the requirements of the bill.

Section 2602, entitled "Assistance capability requirements," con

Requirements," which every telecommunications carrier is required to meet in connection with those services or facilities that allow customers to originate, terminate or direct communications.

The first requirement is expeditiously to isolate and enable the government to intercept all communications in the carrier's control to or from the equipment, facilities or services of a subscribe, concurrently with the communications' transmission, or at any later time acceptable to the government. The bill is not intended to guarantee "one-stop shopping" for law enforcement. The question of which communications are in a carrier's control will depend on the design of the service or feature at issue, which this legislation does not purport to dictate. If, for example, a forwarded call reaches the system of the subscriber's carrier, that carrier is responsible for isolating the communication for interception purposes. However, if an advanced intelligent network directs the communication to a different carrier, the subscriber's carrier only has the responsibility, under subsection (d), to ensure that law enforcement can identify the new service provider handling the communication.

The second requirement is expeditiously to isolate and enable the government to access reasonably available call identifying information about the origin and destination of communications. Access must be provided in such a manner that the information may be associated with the communication to which it pertains and is provided to the government before, during or immediately after the message's transmission to or from the subscriber, or at any later time acceptable to the government. Call identifying information obtained pursuant to pen register and trap and trace orders may not include information disclosing the physical location of the subscriber sending or receiving the message, except to the extent that location is indicated by the phone number. However, if such information is not reasonably available, the carrier does not have to modify its system to make it available.

The third requirement is to make intercepted communications and call identifying information available to government in a format available to the carrier so they may be transmitted over lines or facilities leased or procured by law enforcement to a location away from the carrier's premises. If the communication at the point it is intercepted is digital, the carrier may provide the signal to law enforcement in digital form. Law enforcement is responsible for determining if a communication is voice, fax or data and for translating it into useable form.

The final requirement is to meet these requirements with a minimum of interference with the subscriber's service and in such a way that protects the privacy of communications and call identifying information that are not targeted buy electronic surveillance orders, and that maintains the confidentiality of the government's wiretaps.

The Committee intends the assistance requirements in section 2602 to be both a floor and a ceiling. The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past. The Committee urges against overbroad interpretation of the requirements. The legislation gives industry, in consultation with law enforcement and sub-

ject to review by the FCC, a key role in developing the technical requirements and standards that will allow implementation of the requirements. The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements.

Subsection (b) limits the scope of the assistance requirements in several important ways. First, law enforcement agencies are not permitted to require the specific design of systems or features, nor prohibit adoption of any such design, by wire or electronic communication service provides or equipment manufacturers. The legisiation leaves it to each carrier to decide how to comply. A carrier need not insure that each individual component of its network or system complies with the requirements so long as each communication can be intercepted at some point that meets the legislated requirements.

Second, the capability requirements only apply to those services or facilities that enable the subscriber to make, receive or direct calls. They do not apply to information services, such as electronic mail services, or on-line services, such as Compuserve, Prodigy, America-On-line or Mead Data, or Internet service providers. (The storage of a message in a voice mail or E-mail "box" is not covered by the bill. The redirection of the voice mail message to the "box" and the transmission of an E-mail message to an enhanced service provider that maintains the E-mail service are covered.) Nor does the bill apply to services or facilities that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.

Because financial institutions have major concerns about security and reliability, they have established private communications networks for data transmission traffic such as automated teller machines (ATM), point of sale (credit card) verification systems, and bank wires. Some of these networks are point to point, although many utilize the public network at various points. ATM networks, bankcard processing networks, automated check clearinghouse networks, stock exchange trading networks, point of sale systems, and bank wire transfer, stock transfer and funds transfer systems are all excluded from the coverage of the legislation whether or not they involve services obtained from telecommunications carriers. Private networks such as those used for banking and financial transactions have not posed a problem to law enforcement. There are good reasons for keeping them as closed as possible. These networks are not the usual focus of court authorized electronic surveillance, and the financial information travelling on these networks is already available to law enforcement agencies under the banking laws.

Thus, a carrier providing a customer with a service or facility that allows the customer to obtain access to a publicly switched network is responsible for complying with the capability requirements. On the other hand, for communications handled by multiple carriers, a carrier that does not originate or terminate the message but merely interconnects two other carriers, is not subject to the requirements for the interconnection part of its facilities.

While the bill does not require reengineering of the Internet, nor does it impose prospectively functional requirements on the Internet, this does not mean that communications carried over the